UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/898,365 | 07/03/2001 | Teng Pin Poo | 1601457-0007 | 4356 |

7470 7590 10/05/2011
WHITE & CASE LLP
PATENT DEPARTMENT
1155 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

| EXAMINER | |
|---|---|
| GELAGAY, SHEWAYE | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2437 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 10/05/2011 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

*Ex parte* TENG PIN POO and LAY CHUAN LIM

Appeal 2009-011584
Application 09/898,365
Technology Center 2400

Before ROBERT E. NAPPI, MICHAEL R. ZECHER,
and BRUCE R. WINSOR, *Administrative Patent Judges*.

WINSOR, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from a Non-Final Rejection of claims 1-14, 16-20, and 22-24, which constitute all the claims pending in this application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

## STATEMENT OF THE CASE

Appellants' invention relates to a portable data storage and access control device having biometrics-based authentication capabilities. (Spec. 1.) Claim 1, which is illustrative of the invention, reads as follows:

> 1. A portable device comprising:
>
> a microprocessor;
>
> a non-volatile memory coupled to the microprocessor; and
>
> a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise.

The Examiner relies on the following prior art in rejecting the claims:

| | | |
|---|---|---|
| Bialick | US 6,088,802 | July 11, 2000 |
| Estakhri | US 6,385,667 B1 | May 7, 2002 |
| Bjorn | US 6,799,275 B1 | Sept. 28, 2004 |

Claims 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 17, 18, and 20 stand rejected under 35 U.S.C. § 102(e) as anticipated by Bialick.

Claims 6, 12, 16, 19, and 22 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Bialick.

Claims 3 and 9 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Bialick in view of Bjorn.

Claims 23 and 24 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Bialick in view of Estakhri.

Rather than repeat the arguments here, we make reference to the Briefs (App. Br. filed Mar. 20, 2008; Reply Br. filed Oct. 6, 2008) and the Answer (mailed Aug. 1, 2008) for the respective positions of Appellants and the Examiner.

## ISSUES

The pivotal issues presented by Appellants' arguments are as follows:

### *Rejections for Anticipation by Bialick*

1. Does Bialick disclose "access to [a] non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise," as recited in claim 1?

2. Does Bialick disclose "a biometrics-based authentication module coupled to and controlled by a microprocessor," as recited in claim 1?

3. Does Bialick disclose "the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device," as recited in claim 4?

### *Rejections for Obviousness over Bialick*

4. Does Bialick teach or suggest "a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module," as recited in claim 6?

5. Does Bialick teach or suggest "the biometrics-based authentication module is further configured to encrypt the first biometrics

marker before storing the first biometrics marker in the non-volatile memory," as recited in claim 12?

*Rejections for Obviousness over Bialick and Bjorn*

6. Does Bialick combined with Bjorn teach or suggest "a universal serial bus (USB) plug for coupling the portable device directly to a USB socket of another USB-compliant device," as recited in claim 3?

*Rejections for Obviousness over Bialick and Estakhri*

7. Does Bialick combined with Estakhri teach or suggest "a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer," as recited in claim 23?

## FINDINGS OF FACT

The following enumerated Findings of Fact (FF) are supported by a preponderance of the evidence.

*Bialick*

1. Bialick discloses a peripheral device that has security functionality, a memory device, an input/output device, target functionality, and a host interface (col. 6, ll. 37-40; Fig. 6; *see also* Fig. 4).

2. Bialick discloses that the peripheral device includes a non-volatile memory device used to store computer programs and persistent data, which may be a flash memory device (col. 16, ll. 10-15, Fig. 8, ref. 803).

3. Bialick discloses that an access code can be entered using particular embodiments of target functionality such as a biometric device (col. 10, ll. 58-61).

4. Bialick discloses that an access code may be required before enabling a user to access security functionality (col. 10, ll. 48-52).

5. Bialick discloses that data representing a "user personality" such as restrictions on operation of the peripheral device (e.g., limitations on the types of security operations that can be performed) or specification of operating parameters or characteristics (e.g., cryptographic keys or specification of a particular incarnation of a type of security algorithm, such as a particular encryption algorithm) are stored in a memory device of the peripheral device (col. 10, l. 62 – col. 11, l. 10).

6. Bialick discloses that the access code may be used to access other functionality of the peripheral device and to access and identify the personality of a user (col. 10, ll. 62-65).

7. Bialick discloses that "a single user *can* have multiple personalities; each personality *might, for example,* correspond to a different capacity in which the user acts" (col. 11, ll. 5-10)(emphasis added).

8. Bialick discloses that the peripheral device includes a cryptographic processing device adapted to perform security operations that may be any processor capable of performing the desired operations; in one embodiment, the cryptographic processing device may be a special purpose embedded processor (col. 15, l. 63 – col. 16, l. 7; Fig. 8, ref. 801).

9. Bialick discloses that an interface control device mediates interaction between the host computing device, the target functionality and the cryptographic processing device and that the interface control device, under the control of the cryptographic processing device, can be adapted to enable the peripheral device to assume the identity of the target functionality (col. 16. ll. 40-52; Fig. 8, ref. 802, 807, 801).

10. Bialick discloses that the security mechanism can be configured to perform one or more basic cryptographic functions, such as maintenance of data confidentiality, verification of data integrity, user authentication, and user non-repudiation (col. 5, ll. 22-28).

11. Bialick discloses that the peripheral device may be embodied as a card that can be inserted into a corresponding slot of a computer (col. 5, ll. 41-45; Fig. 3B, ref. 312, 313), such as a PCMCIA card enclosing the security and target functionality as a single physical device in a card like housing (col. 5, ll. 53-57; Fig. 4, ref. 404; see also col. 6, l. 65 – col. 7, l. 2).

12. Bialick discloses that a biometric device may be a fingerprint scanner (col. 14, ll. 16-19).

13. Bialick discloses that where the peripheral device includes a fingerprint scanner positioned on a PCMCIA card, the PCMCIA card may be elongated enabling fingerprints to be scanned while the card is inserted in a host computing device (col. 14, ll. 59-67).

14. Bialick discloses that a peripheral device driver can be implemented so that the user must use an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device (col. 10, ll. 45-48) (*see also* FF 3).

15. Bialick discloses that it may be desirable to ensure that unencrypted data is not stored in a target functionality memory device of the peripheral device (col. 10, ll. 30-35).

16. Bialick discloses that biometric data is stored in a library of data stored in a memory device of the peripheral device (col. 14, ll. 52-58).

17. Bialick discloses that the peripheral device communication interface can be any of a variety of communication interfaces such as a

wireless communications interface, a PCMCIA interface, a smart card interface, a serial interface (such as an RS-232 interface), a parallel interface, a SCSI interface, or an IDE interface (col. 5, ll. 5-10).

*Bjorn*

18. Bjorn discloses a universal serial bus (USB) standard for digital connections in computer systems (col. 2, ll. 58-61).

*Estakhri*

19. Estakhri discloses that PCMCIA and USB are examples of available protocols for attaching peripheral devices to a host computer (col. 5, ll. 34-37).

20. Estakhri discloses a flash memory card capable of being used in a USB, PCMCIA, or ATA IDE operating mode (Fig. 2).

21. Estakhri discloses connecting a flash memory card to a host computer by means of a USB plug (Fig. 1A, ref. 90, 50; Fig. 3, ref. 320, 335, 314).

## ANALYSIS

### *Claims 1, 2, 5, 7, 8, 11, 13, 14, 17, 18, and 20*

Appellants contend that because "Bialick does not disclose a mode in which more than one target functionality is used" (App. Br. 8), "Bialick does not disclose that an access code has to be entered before a user is enabled to access data stored in a non-volatile memory of a portable device" (*id.*). This contention relies on the distinction made by Bialick between "security functionality" and "target functionality" (*id.*). Appellants further contend (App. Br. 9) that Bialick does not disclose "a biometrics-based authentication module coupled to and controlled by a microprocessor," because Bialick discloses “a special purpose processor for performing cryptographic operations” and “biometrics-based user authentication is not a cryptographic operation” (*id.*).

We find the Examiner’s findings (Ans. 3-6) and explanations (Ans. 14-21) to be reasonable and adopt them as our own.

For emphasis only, we note that Appellants’ reliance on the distinction between Bialick’s security functionality and target functionality is unpersuasive. We find Bialick discloses a peripheral device (i.e., “portable device”) that includes a non-volatile memory that is separate from the target functionality of the peripheral device (FF 1, 2) and which may be a flash memory (FF 2). We further find that Bialick discloses that the access code, which may be a biometric code (FF 3) is required to access the security functionality of the peripheral device (FF 4), the personality data (FF 5, 6), and other functionality of the peripheral device (FF 6). A person of ordinary skill in the art would understand that the access code is required to access data and programs related to the security functionality, personality data, or other functionality of the peripheral device that are stored in the non-volatile memory of the peripheral device (*see* FF 1, 2), with access denied otherwise.

Appellants further argue that “the access code used to identify a personality in Bialick cannot be provided by biometric authentication” (Reply Br. 4) because “biometric authentication cannot support a single user having multiple ‘personalities’” (Reply Br. 5). We disagree. Bialick discloses that it is *possible* to assign multiple “personalities” to a single user (FF 7), which we find to be a disclosure of one alternative embodiment, but does not disclose that a single user has multiple personalities in every embodiment.

Appellants also contend that Bialick does not disclose allowing the user access to the personality data because “[s]uch access would allow the user to alter his or her own personality data or even alter the access code entered in the first place . . . defeat[ing] whatever protections the personality data offered” (Reply Br. 5-6). We disagree. Appellants have not directed our attention to any teaching in Bialick that would lead us to conclude that it would be undesirable to permit an *authenticated* user to change his or her own personality data. Additionally, claim 1 does not preclude *access* to the non-volatile memory from reading on the ability to use or view data on the non-volatile memory without the ability to change that data.

For additional emphasis, we note that Appellants’ reliance on the special purpose nature of Bialick’s cryptographic processing unit is also unpersuasive. We find that Bialick discloses that that the processor (i.e., “microprocessor”) may be any suitable processor (FF 8) and the processor controls the biometric device (FF 3) at least through the mediation of Bialick’s interface control device (FF 9). Additionally, we find that Bialick discloses that the security functions controlled by the cryptographic processing unit include controlling the verification of the access codes (i.e., “authentication of the user’s identity”) (FF 8, 10).

We sustain the rejection of claim 1. Independent claim 7 and 17 were argued together with claim 1 (App. Br. 5) and by relying on arguments that parallel those made for claim 1. The arguments made for the patentability of dependent claims 5, 11, 13, and 14 (App. Br. 10-11) rely on, or are substantially the same as, arguments made for claims 1, 7, or 17, or merely point out what the claims recite. *See* 37 C.F.R. § 41.37(c)(1)(vii). Dependent claims 2, 8, 18, and 20 were not separately argued. Accordingly, we also sustain the rejection of claims 2, 5, 7, 8, 11, 13, 14, 17, 18, and 20.

*Claims 4 and 10*

Appellants contend (App. Br. 10) that Bialick does not disclose that the biometrics-based sensor is fitted on one surface of the portable device as recited in claim 4 or integrated into the portable device in a unitary construction as recited in claim 10.

We find the Examiner's findings (Ans. 3) and explanations (Ans. 18-19) to be reasonable and adopt them as our own.

For emphasis, we note that Bialick's PCMCIA card (i.e., "portable device") is a structure that is substantially planar, as illustrated in Bialick's Fig. 3B (*see* FF 11). We find that Bialick discloses that a biometric sensor, such as a fingerprint scanner, is integrated into the PCMCIA card (FF 3, 11, 12, 13) to form a unitary construction. We further find that one of ordinary skill in the art would understand from Bialick's disclosure (FF 11, 13) that in an integrated assembly a fingerprint scanner would necessarily be located on a single planar surface of Bialick's PCMCIA card.

Accordingly, we sustain the rejection of claims 4 and 10.

*Claims 6, 16, and 22*

The Examiner finds that it would be obvious to provide a bypass mechanism to enable a user to bypass the biometric-based authentication in the event of authentication failure by the biometrics-based authentication module, in light of Bialick's disclosure of biometrics-based authentication (FF 3) and authentication by password or PIN (FF 14) (Ans. 7-8). The Examiner explains "[t]his modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick et al., in order to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources" (Ans. 9). The Examiner further explains "[t]his modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick, in order to provide a system that allows access to the peripheral device without biometric-based authentication in the event that the user incorrectly or incompletely applies security operations. (Bialick, col. 8, lines 33-37)." (Ans. 22.)

Appellants contend that "[t]he Examiner has not identified any prior art reference that discloses a microprocessor that provides a bypass mechanism for authentication when a biometrics-based authentication fails" (App. Br. 12). Appellants further contend that "[s]imply suggesting use of a security functionality does not teach or suggest use of a bypass mechanism for authentication when a biometrics-based authentication module fails" (*id.*).

Although we note that claim 6 recites "a bypass mechanism for authentication upon a determination of *authentication failure* by the biometrics-based authentication module" (emphasis added), rather than failure of the biometrics-based authentication *module*, we nonetheless agree with Appellants. Bialick discloses biometrics-based authentication (FF 3) and password or PIN authentication (FF 14) as alternatives, and we find no teaching or suggestion that password or PIN authentication, or any other mechanism, can or should be used to bypass the biometric-based authentication in the event of an authentication failure.

Accordingly, we do not sustain the rejection of claim 6, or of claims 16 and 22, which recite substantially the same limitations as claim 6.

*Claims 12 and 19*

Appellants contend that Bialick does not teach or suggest "the biometrics-based authentication module is further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory" as recited in claim 12 (App. Br. 14).

We find the Examiner's findings (Ans. 8-9) and explanations (Ans. 22-23) to be reasonable and adopt them as our own.

For emphasis only, we find that Bialick discloses encryption of data stored on a memory device of a peripheral device (i.e., "portable device") (FF 10, 15), and that biometric markers are stored as data in a non-volatile memory of the peripheral device (FF 2, 16). We find that a person of ordinary skill in the art would find it obvious to combine the teachings of Bialick to encrypt the biometric marker data stored in the non-volatile memory, and that such a combination, in addition to being suggested by Bialick, as found by the Examiner (Ans. 8, 23), is a combination of familiar elements according to known methods that does no more than yield predictable results. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007).

We sustain the rejection of claim 12 and of claim 19, which was argued on substantially the same basis as claim 12 (*see* App. Br. 14-15).

*Claims 3 and 9*

Appellants contend Bialick combined with Bjorn does not teach or suggest "a universal serial bus (USB) plug for coupling the portable device directly to a USB socket of another USB-compliant device" as recited in claim 3 (App. Br. 15-16). Appellants argue that Bjorn discloses a smart card, which cannot physically support a USB connector (App. Br. 16-17).

We find the Examiner's findings (Ans. 10-12) and explanations (Ans. 23) to be reasonable and adopt them as our own.

For emphasis, we find that Bialick discloses a portable device integrated into a PCMCIA card that is inserted into a PCMCIA socket of another PCMCIA compliant device (FF 11). One of ordinary skill in the art would recognize that Bialick's PCMCIA card necessarily comprises a PCMCIA plug that inserts into the PCMCIA socket of the other device. We further find that Bialick discloses that a variety of communication protocols may be used instead of the PCMCIA protocol (FF 17), and the person of ordinary skill in the art would understand that each protocol has a corresponding apparatus for interconnection of devices.

> The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art.

*In re Keller*, 642 F.2d 413, 425 (CCPA 1981) (citations omitted). We agree with the Examiner that it would be obvious to a person of ordinary skill in the art to combine the USB communication protocol disclosed by Bjorn (FF 18) and corresponding USB plug with Bialick's portable device. Such a combination is a combination of familiar elements according to known methods that does no more than yield predictable results. *See KSR*, 550 U.S. at 416.

Therefore, we sustain the rejection of claim 3 and of claim 9, which was argued on substantially the same basis as claim 3 (*see* App. Br. 16-17).

*Claim 23*

Appellants present arguments for the patentability of claim 23 that are substantially the same as those presented for claims 1, 7, and 17 (App. Br. 17-18) (*see* issues 1 and 2 *supra*). These arguments are unpersuasive for the reasons discussed *supra* regarding claims 1, 2, 5, 7, 8, 11, 13, 14, 17, 18, and 20, and we will not repeat those discussions here. We find, additionally, that claim 23 does not preclude "user data" from reading on Bialick's data representing a user personality (FF 5).

Appellants additionally contend that the combination of Bialick with Estakhri does not teach or suggest a USB plug integrated into the housing without an intervening cable and capable of coupling a unitary portable data storage device directly to a USB socket on a host computer as recited in claim 23 (App. Br. 18-20; Reply Br. 12-15). Appellants further contend that:

> the two references disclose systems geared towards completely opposite objectives. *Bialick* teaches an access control system that serves to restrict access to information stored in a host computer, whereas *Estakhri* teaches an interfacing system that facilitates access to information stored in multiple memory cards. Thus, *Bialick* and *Estakhri* teach two distinct endeavors that seek to achieve opposite results: restricting access to stored information in a host computer versus facilitating access to stored information in multiple memory devices.

(App. Br. 19-20)

We find the Examiner's findings (Ans. 12-14), read together with the Examiner's explanations (Ans. 23-25), to be reasonable and adopt them as our own.

For emphasis only, we find that Bialick discloses a unitary portable data storage device (FF 2, 5) having biometrics capability (FF 3, 12) integrated into a PCMCIA card housing without an intervening cable that is inserted into a PCMCIA socket of another PCMCIA compliant device, such as a host computer (FF 11). One of ordinary skill in the art would recognize that Bialick's PCMCIA card necessarily comprises a PCMCIA plug that inserts into the PCMCIA socket of the other device. We further find that Bialick and Estakhri each disclose that a variety of communication protocols may be used instead of the PCMCIA protocol (FF 17, 19), and a person of ordinary skill in the art would understand that each protocol has a corresponding apparatus for interconnection of devices.

We disagree with Appellants that Bialick and Estakhri teach away from combining the references, as the teachings cited by Appellants are not mutually exclusive or opposite, merely different, and do not criticize, discredit, or otherwise discourage the combination. *See In re Fulton,* 391 F.3d 1195, 1201 (Fed. Cir. 2004). We agree with Examiner that a person of ordinary skill in the art would find it obvious to combine Estakhri's USB operating mode and connector (FF 20, 21) with Bialick's unitary portable data storage device without an intervening cable, *see Keller*, 642 F.2d at 425. Such a combination is a combination of familiar elements according to known methods that does no more than yield predictable results. *See KSR*, 550 U.S. at 416.

Therefore, we sustain the rejection of claim 23. Appellants' arguments for the patentability of claim 24 are substantially the same as those made for claim 23 and are unpersuasive for the same reasons. Accordingly, we also sustain the rejection of claim 24.

## DECISION

The decision of the Examiner to reject claims 1-5, 7-14, 17-20, 23, and 24 is affirmed. The decision of the Examiner to reject claims 6, 16, and 22 is reversed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2010).

AFFIRMED-IN-PART

msc